Discrete Mathematics 56 (1985) 299–303
North-Holland

A CLASS OF DOUBLY EVEN SELF DUAL BINARY CODES

Jacques WOLFMANN

GECT, U.E.R. de Sciences et Techniques, Université de Toulon, 83130 La Garde, France

Received December 1984

We give a construction of an infinite class of doubly even self dual binary codes including a code of length 112. (The study of such a code is closely related to the existence problem of a projective plane of order ten.)

1. Introduction

The doubly even self dual binary codes have been studied extensively [5]. We know, for example, that there exists a class of such codes that is 'good' (in the sense of Shannon theorem) [5], the existence problem of the subclass of extremal codes [5] being always open. On the other hand, it has been shown that if a projective plane of order ten exists, then it may be associated to a binary doubly even (112, 56, 12)-code. For this and the general problem of codes generated by incidence matrices of projective planes, we refer to [1], [2] and [5].

In this paper, we shall construct an infinite class of doubly even self dual binary codes including a code of length 112. We shall use the technique of binary image of an H-code [10] relative to a normal and trace-orthogonal basis [10, 9].

We refer to [5] for the classical notions and results on coding theory.

2. Preliminaries

2.1. *Binary image.*

Let $GF(2^r)$ be the field with 2^r elements and $B=\{b_1, b_2, \ldots, b_r\}$ a basis of $GF(2^r)$ considered as a vector space over GF(2).

If $x=(x_1, x_2, \ldots, x_n)\in[GF(2^r)]^n$, the *binary image* $d(x)$ of x is obtained by replacing each x_i by $(x_i^1, x_i^2, \ldots, x_i^r)$, where $x_i=\sum_{j=1}^r x_i^j b_j$ with $x_i^j\in GF(2)$:

$$d(x)=(\ldots, x_i^1, x_i^2, \ldots, x_i^r, \ldots).$$

It is immediate that if C is a linear (n, k, δ)- code over $GF(2^r)$, then $d(C)$ is a linear (nr, kr, D)-code over GF(2) with $D\geq\delta$.

The following proposition is easy to prove.

Proposition 1. *If* $\{c_i \mid i = 1, \ldots, k\}$ *is a basis of* C *over* GF(2^r) *and* $\{u_j \mid j = 1, \ldots, r\}$ *is a basis of* GF(2^r) *over* GF(2), *then* $\{d(u_j c_i) \mid i = 1, \ldots, k, j = 1, \ldots, r\}$ *is a basis of* $d(C)$ *over* GF(2).

2.2. *Trace-orthogonal basis.*

Definition. A *trace-orthogonal basis* of GF(2^r) over GF(2) is a basis that is orthogonal with respect to the bilinear symmetric non-degenerate form $(x, y) \to \operatorname{tr} xy$ where $x, y \in \mathrm{GF}(2^r)$ and tr is the trace of GF(2^r) over GF(2). That is to say $B = \{b_1, \ldots, b_r\}$ is a trace-orthogonal basis if and only if $\operatorname{tr}(b_i b_j) = \delta_{ij}$ (Kronecker symbol).

If $\langle , \rangle$ denote the usual scalar product in K^s: $\langle a, b \rangle = \sum_{i=1}^{s} a_i b_i$ with $a = (a_1, \ldots, a_s)$, $b = (b_1, \ldots, b_s) \in K^s$, then we easily obtain the following propositions.

Proposition 2. *If* d *is the binary image relative to a trace-orthogonal base, then for all* $x, y \in \mathrm{GF}(2^r)$,

$$\operatorname{tr}(\langle x, y \rangle) = \langle d(x), d(y) \rangle$$

Proposition 3. *If* C *is a self-dual code over* GF(2^r) (*that is* $C^{\perp} = C$), *then* $d(C)$ *is also a self-dual code over* GF(2), d *being the binary image relative to a trace-orthogonal basis.*

We know that trace-orthogonal basis exist in GF(2^r) [4].

2.3. *Normal basis.*

A *normal basis* of GF(2^r) is a basis B formed by all the conjugates of one element:

$$B = \{u, u^2, \ldots, u^{2^i}, \ldots, u^{2^{r-1}}\}.$$

It is well known that normal bases exist in GF(2^r). Moreover if r is odd, then there exists in GF(2^r) a basis that is simultaneously normal and trace-orthogonal.

2.4. *Group algebra* GF(2^r)[G]

Let $G = (\mathrm{GF}(2^m), +)$ be the additive group of GF(2^m). The algebra GF(2^r)[G] is the set of formal linear combinations $x = \sum_{g \in G} x_g X^g$ where $x_g \in \mathrm{GF}(2^r)$ with the following laws of operation:

$$x + y = \sum_g (x_g + y_g) X^g,$$

$$xy = \sum_k \left(\sum_{g+h=k} x_g y_h \right) X^k,$$

$$\lambda x = \sum_g (\lambda x_g) X^g, \quad \lambda \in \mathrm{GF}(2^r).$$

If $G = \{g_0, g_1, \ldots, g_{n-1}\}$ we identify $GF(2^r)[G]$ with $[GF(2^r)]^n$ by the mapping

$$x = \sum_g x_g X^g \to (x_{g_0}, x_{g_1}, \ldots, x_{g_{n-1}}).$$

In this way, each vector subspace in $GF(2^r)[G]$, in particular each ideal, is identified with a linear code of length $n = |G|$ over $GF(2^r)$.

2.5. *H-codes.*

Definition. Let H be a hyperplane in $GF(2^m)$ (a $m-1$ dimensional vector subspace). If $x(=\sum_g x_g X^g) \in GF(2^r)[G]$ verifies the condition $\sum_{g\in H} x_g = \sum_{g\in H} x_g = 1$, the principal ideal (x) generated by x in $GF(2^r)[G]$ is called a *H-code.*

Proposition 4 (Camion [3, 8]). *A H-code C is always self-dual. If C is generated by x, then* $\{xX^g \mid g \in H\}$ *is a basis of C.*

Remark. The H-codes are self-dual codes over an extension of GF(2), consequently their binary images relative to trace-orthogonal basis are self-dual codes over GF(2). In particular, some extended Reed–Solomon codes are H-codes. In this way, we find interesting binary codes and applications to decoding [7–10]. In the following, this method is used to find binary doubly even self-dual codes.

3. A class of binary doubly even self-dual codes

The aim of this work is to prove the following result.

Theorem. *Set* $r = 2^{m-1} - 1$. *Let* $B = \{u, u^2, \ldots, u^{2^{r-1}}\}$ *be a normal and trace-orthogonal basis of* $GF(2^r)$, H *an hyperplane in* $GF(2^m)$, $\tilde{H} = GF(2^m) \setminus H = \{g_0, g_1, \ldots, g_r\}$ *and* $G = (GF(2^m), +)$.

If $x = 1 + X^{g_0} + \sum_{i=1}^{r} (u^{2^{i-1}} + u^{2^i}) X^{g_i}$, *then* $d((x))$, *the binary image of the ideal* (x) *generated by x in* $GF(2^r)[G]$ *relative to the basis B, is a doubly even self-dual code.*

Proof. The proof will be divided into several steps.

(A) (x) *is a H-code.* Indeed we have $\sum_{g\in H} x_g = 1$ and $\sum_{g\in H} x_g = 1 + \sum_{i>1} (u^{2^{i-1}} + u^{2^i}) = 1 + \mathrm{tr}\, u + \mathrm{tr}\, u^2 = 1$. From Proposition 3, we immediately deduce that $d((x))$ is self-dual.

(B) *All elements of a basis of* $d((x))$ *have the same weight.* From Propositions 1 and 4, $\{d(u^{2^j} \times X^g) \mid g \in H, j = 1, 2, \ldots, r\}$ is a basis of $d((x))$. We verify that $w(d(u^{2^j} \times X^g)) = w(d(u^{2^j} x))$ ($w(c)$ is the weight of c), because the map $y \to yX^g$ is a permutation of the components of y. On the other hand, $w(d(u^{2^j} x)) = w(d(ux))$ because, from the very definition of x, the components of $u^{2^j} x$ are obtained by conjugation ($z \to z^2$) from those of ux. The basis B being normal, the components of a^2 in $GF(2^r)$ relative to B are obtained by permuting those of a. Finally, the components of $d(u^{2^j} x X^g)$ are obtained by permuting those of $d(ux)$ and each element of the basis of $d((x))$ has the same weight as $d(ux)$.

(C) *The weight of* $d(ux)$ *is a multiple of* 4. We have

$$ux : (u, 0, \ldots, 0, u, \underbrace{u(u+u^2)}_{x_0}, \underbrace{u(u^2+u^4)}_{x_1}, \ldots, \underbrace{u(u^{2^{r-1}}+u)}_{x_{r-1}}).$$

If $z \in \mathrm{GF}(2^r)$, it is easily shown that $z = \sum_{i=0}^{r-1} \mathrm{tr}(u^{2^i} z) u^{2^i}$ because the basis is trace-orthogonal. Denote by $[i, j]$ the component of x_i relative to u^{2^j}, that is $[i, j] = \mathrm{tr}(u^{2^j} x_i)$. Then we obtain

$$\begin{aligned}[i, j] &= \mathrm{tr}[u^{2^j} u(u^{2^{i-1}} + u^{2^i})] = \mathrm{tr}([u^{2^j} u(u^{2^{i-1}} + u^{2^i})]^{2^{-j}}) \\ &= \mathrm{tr}[u^{2^{-j}} u(u^{2^{i-j-1}} + u^{2^{i-j}})] \quad (-j \text{ computed modulo } r).\end{aligned}$$

This gives

$$[i, j] = [i-j, -j] \quad (-j \text{ computed modulo } r). \tag{1}$$

Now let $X_j = ([0, j], [1, j], \ldots, [r-1, j])$ be the vector whose components are respectively those of $x_0, x_1, \ldots, x_{r-1}$ relative to u^{2^j}. From (1), we deduce

$$w(X_j) = w(X_{-j}) \quad (-j \text{ computed modulo } r). \tag{2}$$

But, the word $d((x_0, x_1, \ldots, x_{r-1}))$ has the same weight as $(X_0, X_1, \ldots, X_{r-1})$, because each of these words contains the components of x_i relative to the basis B.

Otherwise, we know that $\sum_{i=0}^{r-1} x_i = 0$, $d((x))$ being self-dual. Hence for all j, $w(X_j) = 0 \pmod 2$. Thus from (2) we have $w(X_1, X_2, \ldots, X_{r-1}) = 0 \pmod 4$. Finally,

$$\begin{aligned}w(ux) &= w(u, 0, \ldots, 0, u) + w(x \cdots x_{r-1}) \\ &= 2 + w(X_0) + w(X_1, X_2, \ldots, X_{r-1}) \\ &= 2 + w(X_0) \pmod 4.\end{aligned}$$

To conclude the proof, we now show that $w(X_0) = 2$. We have

$$\begin{aligned}X_0 &= ([0, 0], [1, 0], \ldots, [r-1, 0]) \\ &= (\mathrm{tr}(u^2(u+u^2)), \mathrm{tr}(u^2(u^2+u^4)), \ldots, \mathrm{tr}(u^2(u^{2^{i-1}}+u^{2^i})), \ldots).\end{aligned}$$

But $\mathrm{tr}(u^2(u^{2^{i-1}}+u^{2^i})) = \mathrm{tr}\, u^2 \cdot u^{2^{i-1}} + \mathrm{tr}\, u^2 u^{2^i} = \delta_{2,i-1} + \delta_{2,i}$. This number is equal to 1 only in the cases $i = 2$ and $i = 3$, and it is zero in the other cases. Hence $w(X_0) = 2$ and the theorem is proved. □

4. Commentaries

For a fixed m, the length of the code $d((x))$ is $n = 2^{2m-1} - 2^m$.

In the case $m = 3$, we have $n = 24$ and we may verify that we obtain a (24, 12, 8)-code which is therefore equivalent to the Golay code and the construction is equivalent to the one used in [8] and [7] (see [10]).

In the case $m = 4$, we have $n = 112$. It may be shown that this code of length 112 which is doubly even and self-dual cannot be the one associated to an

hypothetical projective plane of order 10. Nevertheless, if such a plane exists, the associated doubly even self-dual code may be transformed into the one we have found here by means of some operations. But this will be the purpose of another paper.

References

[1] E.F. Assmus Jr., On the possibility of a projective plane of order 10, Part II in Algebraic Theory of Codes II, Final Report, GTE-Sylvania, Contract No F19628-69-C-0068 (1970).
[2] E.F. Assmus Jr., et al., Self-orthogonal Steiner systems and projective planes, Math. Z. 138 (1974) 89–96.
[3] P. Camion, Etude de codes binaries abeliens modulaires auto-duaux de petites longueurs, Rev. CETHEDEC 79(2) (1979) 3–24.
[4] A. Lempel, Matrix factorization over GF(2) and trace orthogonal basis of GF(2), SIAM J. Comput 4 (1975) 175–186.
[5] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes (North-Holland, Amsterdam, 1977).
[6] F.J. MacWilliams, N.J.A. Sloane and J.G. Thompson, On the existence of a projective plane of order 10, J. Combin. Theory Ser. A 14 (1973) 66–78.
[7] G. Pasquier, The binary Golay code obtained from an extended cyclic code over F_8, European J. Combin. 1 (1980) 369–370.
[8] J. Wolfmann, A new construction of the binary Golay code (24, 12, 8) using a group algebra over a finite field, Discrete Math. 31 (1980) 337–338.
[9] J. Wolfmann, A permutation decoding of the (24, 12, 8) Golay code, IEEE Trans. Inform. Theory 29 (1983) 748–750.
[10] J. Wolfmann and G. Pasquier, A class of binary self dual codes, Rapport interne GECT, Université de Toulon.